Efficient Public-Key Certificate Revocation Schemes for Smart Grid

Mohamed M. E. A. Mahmoud\textsuperscript{1}, Member, IEEE, Jelena Mivic\textsuperscript{2}, Senior Member, IEEE, and Xuenin (Sherman) Shen\textsuperscript{3}, Fellow, IEEE

\textsuperscript{1}Department of Electrical and Computer Engineering, Tennessee Tech University, Cookeville, Tennessee, 38505, USA
\textsuperscript{2}Department of Computer Science, Ryerson University, Toronto, Ontario, M5B 2K3, Canada
\textsuperscript{3}Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada

Abstract—The public key cryptography will play an essential role in securing the smart grid communications. For the secure use of the public key cryptography, an efficient and secure certificate revocation scheme specially tailored to smart grid architecture should be adopted. In this paper, we study certificate revocation in smart grid and design efficient and scalable certificate revocation schemes. The schemes have different security strengths and require different overhead levels. We also propose an efficient certificate revocation scheme for pseudonymous public key infrastructure using compressed certificate revocation lists. Analytical results demonstrate that using revocation schemes is essential for securing smart grid, and the proposed schemes are secure. Moreover, simulation results demonstrate that the proposed schemes require low overhead.

Index terms: Public key cryptography, smart grid communication security, and certificate revocation schemes.

I. INTRODUCTION

The 2005 Houston blackout \cite{1} has demonstrated that the power grid was not able to isolate the blackout and recover from it due to the lack of sufficient sharing of phasor measurement data. This incident demonstrates that the existing power grid needs to be modernized to avoid the devastating effects of a cascading failure of the electricity grid. During a blackout, millions of houses will be deprived of electricity, the economic losses will be heavy, electric trains will be halted, and many traffic signals will not work causing car collisions.

Traditional power grid is featured with one-way power transmission (from generation plants to consumers) and demand-driven response. Smart grid \cite{1} has been envisioned as a promising evolution to the existing power grid. It integrates information and communication systems into electric transmission and distribution networks. The next generation power grid will allow two-way transmission of power and flow of information. It aims to provide improved reliability (e.g., self-healing) and efficiency (e.g., low-cost power generation and delivery). It controls intelligent appliances at consumers to save energy, reduce cost, and increase reliability and efficiency.

Moreover, according to the Electric Power Research Institute (EPRI), one of the main challenges facing the smart grid deployment is related to cyber security of the grid \cite{2}. The smart grid communication networks are vulnerable to security breaches due to the network scalability, open architecture, and the lack of physical protection for the network devices. These attacks will target the network availability and proper operation, causing widespread power outage. No responsible government will allow the deployment of the smart grid if there is a little chance of cyber attacks launched by an opponent country that can bring down the nation’s power system.

The public key cryptography (PKC) will play an essential role in securing the smart grid communications. PKC can ensure messages’ authenticity and integrity \cite{3}. It can also ensure non-repudiation of sending a message or its content, which is essential to enforce accountability. Public key cryptography can be used to enforce access control to protect the proper operation of the grid. In PKC, digital certificates are usually used to bind the certificate holder’s identity with its public key. When a certificate is issued, its validity is limited by an expiration date. However, there are circumstances that necessitate revoking a certificate before the expiration date. These circumstances will be discussed in details in Section II-B. Compromised nodes can be excluded from the network by revoking their certificates because the messages sent with using revoked certificates are ignored.

The existing public-key certificate revocation schemes cannot be used efficiently and effectively for smart grid because of the grid’s unique characteristics. These characteristics include complexity, scalability, the nodes’ immobility, and the large geographical spread of the communication network. Therefore, the smart grid’s unique characteristics necessitate designing certificate revocation schemes tailored to the smart grid. Although the smart grid has recently gained extensive attention, the design of a public key certificate revocation scheme that can effectively handle hundreds of millions of certificates has not yet been well studied. In this paper, we study certificate revocation in smart grid and propose efficient and scalable certificate revocation schemes. These schemes have different security strengths and require different overhead levels.

Moreover, certificate revocation can be achieved by disseminating Certificate Revocation Lists (CRLs) that contain the identifiers of the revoked certificates. To verify the status of a certificate, each node has to check if the certificate’s identifier is in the list. However, this solution is not scalable or efficient especially for pseudonymous public key infrastructure (PPKI). In PPKI, each node should hold a large number of certificates with different public keys and pseudonyms to preserve the nodes’ communication privacy. In PPKI, it is expected that the CRLs will be very long because of the large number of certificates in the system. We propose a compressed CRL-based revocation scheme for PPKI. A large set of certificates whose identifiers satisfy some keyed hash-chain based serial relationship can be revoked by releasing the key used to generate the chain and the first identifier of the revoked certificate list.

Our main contributions in this paper can be summarized as follows. (1) We study certificate revocation in smart grid; (2) we design efficient and scalable certificate revocation schemes specifically tailored for smart grid; and (3) we propose efficient certificate revocation scheme for pseudonymous public key infrastructure using compressed certificate revocation lists.

The remainder of this paper is organized as follows. Section II presents the system models, the certificate revocation motivations, and the issues that should be considered when designing a certificate revocation scheme for smart grid. Section III presents our certificate revocation schemes. Performance and security evaluations are given in Section IV. The related works are discussed in section V, followed by conclusions in Section VI.
II. PRELIMINARY

A. System Models

Fig. 1 shows the considered smart grid architecture. The electric power is generated at the power plants and supplied to consumers via transmission and distribution substations. The transmission substations deliver power from the plants over high voltage transmission lines to the distribution substations. The distribution substations transform the electric power into medium voltage level and then distribute it to the building-feeders. The medium voltage level is converted by the building-feeders into a lower level usable by consumer appliances.

 Supervisory control and data acquisition (SCADA) can communicate with control centers and smart grid devices. These devices include substation devices, pole-top equipments, smart meters and in-house devices, etc. SCADA monitors power distribution equipments in substations and in the feeders and determine whether any actions should be taken to improve reliability and efficiency, or respond to emergencies. SCADA also monitors and controls equipments in power transmission substations. It monitors the health of the transmission system and takes corrective actions within a few milliseconds such as tripping circuit breakers if power system anomalies are detected.

 Consumers are the parties that pay for electrical service. Smart meters are two-way communication devices deployed at consumers premise. By using smart meters, the utility companies will periodically receive measurements for billing and for grid management purposes. The grid provides consumers with real-time pricing of electricity to help them to modify their power consumption to pay less and help utilities achieve necessary load reductions, e.g., shift power use from peak times to non-peak times. Distribution/transmission automation within substations involves monitoring and controlling equipments in distribution/transmission substations to enhance power system reliability and efficiency.

B. Certificate Revocation Motivations

When a certificate is issued, its validity is limited by an expiration date. However, there are several situations that necessitate certificate revocation before expiration [4]. Thus, verification the expiration of a certificate is necessary but not sufficient evidence for its validity. A check is required to determine a certificate revocation status. Certificate revocation is the act of invalidating the certificate before the expiration. When a certificate is revoked, all the messages authenticated by the certificate should be ignored. This means without holding a valid certificate, a node is excluded from the grid’s communication network. Strong motivations that necessitate adopting a revocation scheme to secure smart grid are discussed below:

1. Key compromise: The private key of the certificate holder or the certificate authority (CA) that issued the certificate has been compromised or is suspected to be compromised.

2. Loss of security token: The private key might be stored in a smart card or USB device and the certificate holder (e.g., an employee) has lost it. Without revoking the certificate, an attacker can retrieve the private key and sends messages under the name of the employee, e.g., to sabotage or causing chaos in the grid.

3. Change of affiliation or privilege: Certificates are required for employees to use the grid’s communication network. An employee’s certificate is not only associated to his identity, but also to his privileges and permissions. Thus, if an employee is promoted or transferred to a different position or his contract has been terminated early, his certificate must be revoked. This is because some of the certificate’s data has to be changed such as the privilege, the domain name of the entity and the certificate holder’s affiliation.

4. End of certificate’s purpose: The purpose of the certificate for which it was issued does not exist anymore. A certificate may be issued for a temporary purpose, e.g., if damage happens in the system, the hydro company can set up makeshift devices such as collectors to collect electricity readings. These devices are not further required after repairing the infrastructure.

5. Malicious behavior: If the system loses trust in a device, e.g., due to evidence of malfunction or malicious behavior, the system must promptly revoke the certificate of this device to protect the network proper operation. Once this is done, messages from this device will be ignored.

6. Change of security policy: Certificate revocation is necessary when the CA does not work under its defined policy anymore, e.g, it ceases to support certificate services.

7. Defective devices: The certificates of defective devices that are removed from service will need to be revoked. Otherwise, attackers can use their keys to launch attacks.

C. Certificate revocation scheme’s design guidelines

Certificate revocation schemes are generally evaluated based on the following metrics [5]:

1. Overhead: The overhead of revoking a certificate and checking a certificate status should be minimal. Several metrics can be used to measure this overhead such as the communication overhead (or bandwidth requirement), storage area, and the computation cost on the CA and the network nodes. The smart grid will involve communication over a variety of channels with varying bandwidths. Low bandwidth channels will be too slow to disseminate large certificates revocation information. Some devices such as residential meters and in-home devices may be limited in their computational power and/or ability to store large data. Each time a signed message is received, the verifier has to check if the certificate is revoked. The latency of this check should be minimized to expedite message authentication.

2. Scalability: This metric depicts how a revocation scheme scales up in large networks. A scheme with a large number of potentially revocable certificates is expected to require more resources comparing to small scale schemes.

3. Robustness: This metric measures the scheme’s ability to resist potential threats. Availability is one way to measure robustness. If the scheme needs online server, the availabil-
ity of the certificate revocation information will rely on the availability of the server. If the server goes down, the nodes will not be able check the certificates revocation status.

4. **Vulnerability period (or revocation latency):** This is the time interval between the moment when a revocation decision is made and when the revocation information becomes available to all the nodes, i.e., when revocation is indeed implemented. Good certificate revocation scheme should minimize this period because during this period, the messages sent by revoked certificates will be accepted. The vulnerability period should particularly be minimized in case of revoking high-privilege certificates. This is because they have enough privileges to cause substantial damage.

III. **CERTIFICATE REVOCATION SCHEMES**

Designing an efficient certificate revocation scheme for smart grid is a challenge due to the massive scale of the network nodes. Novel and innovative solutions are required to manage certificate revocation. In this section, we present five certificate revocation schemes called short-lived-certificate based, tamper-proof-device based, online certificate status server based, certificate revocation list (CRL) based, and compressed CRL based.

A. **Short-lived-certificate based scheme**

This scheme makes use of the fact that a certificate is automatically revoked after it expires. Short-lived certificates will be self-revoked after short time. If the CAs issue short-lived certificates, each node will need to contact the CAs to renew its certificate every short time. The CAs can revoke certificates by denying renewing them.

B. **Tamper-proof-device based scheme**

The main idea behind this scheme is that certificates can be revoked by deleting the associated private keys. Without the private keys, the certificates’ holders cannot compute valid signatures [6] despite of having unexpired certificates. Tamper-proof device (TPD) is installed in each node, and the device is secure enough to resist manipulation. TPD stores the node’s private key, and performs security functions such as signature and verification operations.

To revoke a certificate, the CA sends Certificate Revoke Command (CRC) message to the TPD of interest to delete the private key. This message contains the identities of the CA and the device, a timestamp, the identifiers of the certificates to be revoked, and the CA’s signature on the message. The message should be encrypted either by a symmetric key or the device’s public key to prevent attackers from knowing the purpose of the message and dropping it before it reaches the TPD. Since only the TPD can decrypt the message, attackers will not block it. The CA’s signature enables the TPD to verify the authenticity and integrity of the message. The CRC message will have the following format:

\[
\text{CA} \rightarrow \text{TPD}_U : \text{ID}_{CA}, E_y(\text{REVOKE}, \text{Ts}, \text{Cert}_{ID}s), \text{Sig}_{CA}(E_y(\text{REVOKE}, \text{Ts}, \text{Cert}_{ID}s))
\]

Where ID_{CA} is the identity of CA and \(E_y(X, Y, Z)\) denotes the encryption of “X, Y, Z” with the key K. REVOKE indicates the message type, Ts is timestamp, and Cert_{ID}s is the identifiers of the certificates to be revoked. Sig_{CA}(Y) is CA’s signature on Y. When TPD_U receives the message, it verifies the CA’s signature, and decrypts the message. It sends back a Certificate Revocation Acknowledgment (CRA) message to confirm performing the certificate(s) revocation. The CRA message has the following format:

\[
\text{TPD}_U \rightarrow \text{CA} : \text{ID}_u, E_y(\text{REV_CONF}, \text{Ts}, \text{Cert}_{ID}s), \text{Sig}_u(E_y(\text{REV_CONF}, \text{Ts}, \text{Cert}_{ID}s))
\]

Where ID_u is the identity of node U, REV_CONF indicates that the message type is revocation confirmation. Sig_u(Y) is node U’s signature on Y. After sending the message, node U immediately deletes the private keys of the revoked certificates.

C. **Online certificate status server based scheme**

In this scheme, an online and interactive certificate status server is used. The server stores updated revocation information for the certificates of interest. These certificates are the ones needed by the nodes in the server’s domain. The verification of the certificates status can be done through a request/response messages. When a client (a node) needs to check the status of a certificate, the CA sends a certificate revocation list (CRL) based scheme.

A certificate-revocation-list based scheme

In this scheme, certificate revocation list (CRL) is used to distribute certificate revocation information. A CRL is a digitally signed and time stamped black list of the certificates that have been revoked. For verifying a certificate’s revocation status, the certificate is revoked if its identifier is found in the CRL, otherwise it is not revoked. A CRL is periodically issued by each CA to list the identifiers of the revoked certificates that are issued by the CA. Each node should always keep the most up-to-date version of CRL, otherwise, it may accept messages sent with using revoked certificates.

A CRL message contains the version, the issuer, the serial number, issuing date, expiration date, and the complete list of the revoked (and not yet expired) certificates’ identifiers together with their dates of revocation and the revocations’ reasons (may be unspecified). The message also contains the issuer’s digital signature on the message and the algorithm used to generate the signature. The complete format of a CRL message sent by CA_i is indicated in Fig. 2. The digital signature can guarantee the integrity and authenticity of the CRL. It makes no sense to append expired certificates to the CRL since expired certificates are not accepted by the nodes.
To verify the CRL message, each node has to perform the following checks: (1) verify the CA’s signature, (2) ensures that the CRL’s serial number is the expected one, (3) checks that the CRL has arrived at the expected time, and (4) checks that the certificates declared as revoked in the last CRL (and not yet expired) are included in the current CRL.

The CA attaches the certificate revocation reason to the CRL because it can resolve some problems. For example, consider two certificates Cert₁ and Cert₂ having the same public and private keys are issued to one subject by two different CAs called CA₁ and CA₂, respectively. The problem arises if CA₁ revokes Cert₁, and CA₂ says nothing about Cert₂. This problem could be resolved if the reason of revocation is known. For example, if revocation reason is key compromise, all other certificates with the same public–private key pair should also be revoked. However, it the revocation reason is that the subject is no longer affiliated with CA₂, the revocation of Cert₁ should not impact the status of the certificate Cert₂.

The smart grid will implement different systems with different security/overhead requirements. It is not expected that all the certificates will have the same lifetime. Determining a good certificate lifetime will help reduce the CRL size. This is because a revoked certificate’s identifier should stay in the CRL until it expires. A good certificate lifetime should depend on the longevity of its purpose. For example, when certificates are issued to employees whose employment status or duties may change every few years, it would be appropriate to issue certificates with relatively short lifetime, so that in case of revocation, the certificates will stay in the CRL for a short time until expired. Some certificates may be issued to devices that are deployed with the intent to keep them operational for many years, and these devices are housed in a secure environment and have low failure likelihood. In this case, the certificates’ lifetime can be long as the probability of revoking them is low.

CRL-based certificate revocation schemes are widely used in many systems and networks [7]. However, using CRL-based revocation scheme in smart grid is a real challenge because the number of devices in smart grid will be in millions. The CRL size is expected to grow extremely large which may result in large communication overhead to distribute the CRLs and large storage area to store them. The CRLs can be updated and distributed more frequently when the overhead is acceptable. This can make the CRLs fresher and the vulnerability period shorter. Therefore, novel and innovative techniques are needed to make the use of CRL in smart grid efficient. In addition to determining a good certificate’s lifetime to reduce the CRL size, two techniques can be used called incremental CRL (I-CRL) and partitioned CRL (P-CRL).

I-CRL technique can reduce the size of the CRL updates. I-CRL is a short CRL that provides incremental information about the certificates whose status have changed since the last update. The devices should cache the base CRL (the complete list) and adds to it the new certificates revoked in the following updates. If a certificate is revoked in one CRL message, it will not be resent in the next messages. Information about revoked certificates should be stored in the devices until they expire. Therefore, I-CRL will be significantly shorter than a complete CRL, allowing a higher update frequency.

In mobile networks, any two nodes can communicate because of the nodes mobility. In smart grid, the nodes will only communicate with a limited number of other nodes due to the static nature of the network. This means that the nodes do not need the revocation information of all the certificates, but only the certificates’ of interest. P-CRL technique can much reduce the overhead by distributing the revoked certificate of interest instead of all the revoked ones. If CRL contains all revoked certificates, a node’s P-CRL can be defined as a subset of CRL that contains revocation information for the node’s certificates of interest. The size of P-CRL is much shorter than the CRL.

To implement the P-CRL technique, each node should register its certificates of interest with the CA. In an ideal case, the certificate authority creates the P-CRLs that only contain the nodes certificates of interest. However, this high level of granularity will impose huge overhead on the CA for composing the P-CRLs because a large number of signatures will be needed. To reduce the overhead, P-CRL can be composed for the certificates of interest of a group of nodes, e.g., in one geographic region, in such a way that can keep the P-CRL size acceptable with reasonable overhead on the CA. What promotes this idea is that the function of many nodes in the smart grid will be identical, i.e., a group of devices in one neighborhood will have identical or much overlapped certificates of interests. It is worth mentioning that, merging both incremental and partitioned CRLs in one technique called IP-CRL can boost the efficiency.

\[
\begin{align*}
H^{(0)} = R \\
H^{(0)} = h(K, H^{(0)}) \\
H^{(0)} = h(K, H^{(0)}) \\
\vdots \\
H^{(n)} = h(K, H^{(n)}) \\
\vdots \\
H^{(n+1)} = h(K, H^{(n+1)}) \\
\vdots \\
\end{align*}
\]

\[
\begin{aligned}
& H^{(0)} = h(K, R) \\
& H^{(n)} = h(K, H^{(n)}) \\
& 1 \leq i \leq S, \text{ where } S \text{ is the size of the hash chain.}
\end{aligned}
\]

\[
\text{Without knowing } K, \text{ linking the hash chain elements is infeasible.}
\]

\[\text{From Fig. 3, to revoke a certificate series, the CA releases the first identifier in the series } H^{(0)}, \text{ the number of revoked certificates } (n), \text{ and the key used to create the chain. The nodes can compute the complete list of revoked certificates’ identifiers by iteratively hashing the first hash value } n \text{ times with using } K.\]

\[\text{Fig. 3: C-CRL based scheme.}\]
IV. DISCUSSIONS AND EVALUATIONS

In our opinion, one certificate revocation scheme will not be enough to satisfy the overhead/security requirements of all systems in smart grid. For example, revoking a highly-privileged node’s certificate should be done in short time, but revoking less important nodes’ certificates can sustain some delay.

A. Short-lived-certificate based scheme

Comparing to the CRL-based scheme, short-lived-certificate based scheme can save the overhead of distributing CRLs. This scheme can also minimize message authentication delay because it minimizes certificate status check latency. Instead of checking a certificate’s expiration and revocation, only expiration check is required because unexpired certificate is also unrevoked. There is an obvious tradeoff between the overhead and the revocation latency. Short certificate lifetime can reduce the revocation latency, but with more frequency of certificate renewals. On the contrary, long certificate lifetime will give attackers more time to operate without being revoked, but with lower overhead on the CA. This overhead may not be acceptable if the scheme is used on a large scale.

This scheme is suitable for the applications that require fast message authentication. If an application requires immediate revocation of misbehaving nodes to decrease the time window these nodes can jeopardize the proper operation of the grid, other schemes should be solicited. This scheme can suit the nodes that have uncritical privileges that do not enable them to take critical actions, so that even if the nodes are compromised they cannot launch serious attacks. The scheme is also proper for the cases that it is hard or improbable to compromise the nodes’ keys. It may not be proper for smart meters or field devices because they are unattended and attackers have full access to them, but it can be used in substations or SCADA.

B. Tamper-proof-device based scheme

The main advantage of this scheme is the low communication and computation overhead. Only a couple of messages are required to revoke certificates. The low overhead makes the scheme more scalable than short-lived-certificate based scheme. Verifying a certificate revocation status is overhead free because if a message’s signature is valid, the certificate is unrevoked. This can expedite message authentication. Another important advantage is the very low revocation latency. Certificates are revoked instantly after receiving a CRC message. However, the drawback of this scheme is that a secure tamper proof device may be expensive, so a widespread use of this scheme may not be cost efficient.

This scheme can meet the needs of some systems in the grid. It can be used in SCADA because unlike meters and field devices, the SCADA devices are physically protected, i.e., attackers will not have full access to the devices. This can reduce the attackers’ ability to manipulate the tamper proof device, and provide more confidence in the robustness of the TPD. Some sensitive parts of SCADA may need fast revocation especially the highly privileged nodes.

One signing operation and one symmetric-key encryption are required to compose a CRC or CRA message. One verifying operation and one symmetric-key decryption are required to verify a CRC or CRA message. In order to estimate the required computational times and energy to compose and verify a CRC or CRA message, we have implemented 1,024-bit RSA public key cryptosystem and 128-bit AES symmetric-key cryptosystem with using Crypto++ library [14] and 1.6 GHz Intel processor. The signature size is 128 bytes and the signing and verifying operations require 15.63 ms and 0.53 ms, respectively. The AES encryption/decryption operations require 1.52 µs/16 bytes. A node identity, message type, timestamp, and one certificate identifier require four, one, five, and five bytes, respectively.

From [15], the energy consumption for AES is 1.21 µJ per byte, and the energy consumptions for RSA signing and verifying operations are 546.5 mJ and 15.97 mJ, respectively. The CRC and CRA message size is 148 bytes. The computational delay and energy consumption for composing a CRC or CRA message are 15.64 ms and 550 mJ, respectively. The computational delay and energy consumption for verifying a CRC or CRA message are 0.55 ms and 16.2 mJ, respectively.

C. Online certificate status server based scheme

This scheme requires no storage in the nodes, but it does require the always-available communication link to the server. Obviously, the server is a single point of failure, i.e., the nodes cannot check the status of the certificates if the server is out of service. The server should be fully secure and tamper resistant. In addition, the scheme does not scale well. One server cannot serve many nodes and deploying many servers is costly.

The scheme can reduce the vulnerability period provided that the server keeps the freshness of the revocation information. However, if the certificates of interest belong to different CAs, the server has to frequently contact the CAs to ask for updates. This overhead can be reduced by integrating this scheme with CRL-based scheme. In this case, the server stores the recent CRLs published by the CAs. The nodes can acquire the certificates’ revocation status without the need to store a complete CRL. This is very beneficial if it is inefficient to store CRLs in the nodes because of limited memory or long CRLs. This scheme is suitable for unscalable systems that can provide physical protection to the server such as SCADA and substations.

D. CRL based scheme

In this scheme, it is not efficient to compose and distribute an updated CRL momentarily after a certificate is revoked, because this will impose a huge overhead on the system. Instead, the CA has to wait until it accumulates a number of revoked certificates and then release them as a batch. This means there is always a delay between making revocation decision and executing it. CRL-based scheme is inappropriate for the applications that require short vulnerability period because the inherent cost of CRL generation and distribution prohibits timely distribution of revocation information. This scheme has an interesting feature for smart grid that is an offline certificate revocation check.

In P-CRL, each CA groups the full CRL into a series of partitioned CRLs that contain the certificates of interest of a group of nodes. This partitioning should be done in such a way that decreases the number of partitioned CRLs with acceptable overhead on the CA. It is possible that one certificate is included in more than one group. For example, if the full CRL of a CA has 10,000 revoked certificates and a node’s list of revoked certificates of interest is only 50, without partitioning, the node will receive 9,950 unneeded certificates, but with partitioning the P-CRL size will be between 50 and 9,949.

Partitioning is more efficient when the degree of overlapping among the nodes’ certificates of interest is high, i.e., fewer and shorter P-CRLs. This can be applicable to the field sensor nodes. However, using P-CRL may not reduce the overhead a lot in some situations, e.g., a substation has a large number of certificates of interest because it communicates with a large number of nodes.
number of devices. In this case, the substation can receive multiple P-CRLs that cover all its certificates of interest, or it may revert to a different certificate revocation scheme.

For C-CRL based scheme, the size of the certificate revocation list is linear with the number of revoked certificate series, irrespective to the number of revoked certificates each series may have. Only a single entry needs to be added to the C-CRL to revoke a series of certificates. By using this scheme, the CAs not only provide the nodes with enough certificates for privacy preservation, but also keep the size of CRLs reasonable.

The unrevoked certificates’ identifiers are unrelated without knowing a secret key. This unlinkability property is important to preserve privacy. Using unkeyed hash chain will provide less privacy preservation because attackers can link the unrevoked certificates using hashing operations. A secure one-way keyed hash function should satisfy the following properties:

1) The function’s input has an arbitrary length, but the output hash value has fixed-length.
2) Given X and K, it is possible to compute h(K, X), but given h(K, X) and K, it is infeasible to compute X. Given X, it is infeasible to compute h(K, X) without knowing K.
3) Given X and K, it is computationally infeasible to find $X' \neq X$ such that $h(K, X') = h(K, X)$.

Fortunately, there are several secure and efficient hash functions. SHA-1 has 20 byte hash value’s length and can process 16.79 Mega bytes per second and consumes only 0.76 µJ per byte as given in [9].

V. RELATED WORK

In [10], M. Qiu et al. measure the energy consumptions of various security algorithms using energy-constrained nodes. They propose a group of code optimization methods to increase the energy consumption efficiency of different security algorithms. The authors also propose an array of principles on using security algorithms in smart grid communication networks, such as cryptography selection and parameter configuration.

In [11], H. Guo et al. propose a batch authentication protocol for vehicle to smart grid communication. Instead of verifying each packet for each individual vehicle, the aggregator waits for some time to receive multiple responses from a batch of vehicles. The aggregator verifies the received responses by only one signature verification. It then broadcasts a signed confirmation packet to the batch of vehicles with only one signature.

Inspired by the fact that electricity usage data is small in size and multi-dimensional in nature, R. Lu et al. [12] propose an efficient privacy-preserving power consumption data aggregation scheme. For data sent from smart meters, data aggregation is performed directly on ciphertext at local gateways without decryption, and the aggregation result of the original data can be obtained at the operation center. Due to reducing the overhead, data can be efficiently reported to smart grid operation center at a high frequency for real-time monitoring and control.

M. Fouda et al. [13] propose a lightweight message authentication scheme for securing smart grid communications. The smart meters can first achieve mutual authentication and establish the shared session key with Diffie-Hellman exchange protocol. Then, with the shared session key between smart meters and hash-based authentication code technique, the subsequent messages can be authenticated in a lightweight way.

However, although securing smart grid has recently gained extensive attention, studying certificate revocation has not been well studied yet.

VI. CONCLUSIONS

In this paper, we have studied certificate revocation in smart grid and developed efficient and scalable certificate revocation schemes. We have shown that these schemes have different features and can be appropriate for different parts in the grid. We have also proposed an efficient certificate revocation scheme for pseudonymous public key infrastructure using compressed certificate revocation lists. Analytical results have demonstrated that using revocation schemes is essential for securing smart grid, and the proposed schemes are secure. Moreover, simulation results have demonstrated that the proposed schemes require low overhead.

REFERENCES